BCC FACULTY AND STAFF POLICY

ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

In applying for access to any BCC computer network, on-campus access to the Internet connection, FAX, or Long Distance Authorization (aka "information technology resources" or "College ITRs"), the applicant accepts the following conditions:

I. POLICY APPLICATION

This document constitutes a College-wide policy intended to allow for the proper use of all College ITRs, effective protection of individual users, equitable access, and proper management of those resources. This policy applies to the entire College Network and all related equipment and is intended to supplement, not replace, all existing laws, regulations, agreements, and contracts that currently apply to these services.

Access to College owned or operated ITRs imposes certain responsibilities on users and is granted subject to College policies and state and federal laws. Appropriate use should always be legal, ethical, reflect academic honesty and community standards, and show restraint in the consumption of shared resources. All use of these services should demonstrate respect for intellectual property, data ownership, system security, and individuals' rights to privacy and to be free from intimidation, harassment, and unwarranted annoyance.

II. ACCEPTABLE USE

Acceptable use of the College's ITRs by authorized users includes usage for academic, educational or professional purposes that are directly related to official College business and in support of the College's Mission. "Authorized users" are current BCC faculty or staff members.

III. UNACCEPTABLE USE

Unacceptable uses of the College's ITRs, which shall amount to a violation of this policy, shall include, but not be limited to, the following:

- For any illegal act, including violation of any criminal or civil laws or regulations, whether state or federal;
- For any political purpose;
- For any commercial purpose;
- To send threatening or harassing messages, whether sexual or otherwise;
- To access, share or download sexually explicit or obscene material;
- To infringe any intellectual property rights;
- To gain, or attempt to gain, unauthorized access to any computer or network;
- For any use that causes interference with or disruption of network users and resources, including propagation of computer viruses or other harmful programs;
- To intercept communications intended for other persons;
- To misrepresent either the College or a person's role at the College;
- To distribute chain letters;
- To access online gambling sites; or
- To libel or defame any person.

IV. DATA CONFIDENTIALITY

In the course of performing job related duties, a user of the College's ITRs may have access to confidential or proprietary information, such as personal data about identifiable individuals or commercial information about business organizations. Under no circumstances is it permissible for employees or contractors to acquire access to confidential data unless such access is required by their jobs. Under no circumstances may employees or contractors disseminate any confidential information that they have rightful access to, unless such dissemination is required by their jobs and authorized.

V. INTELLECTUAL PROPERTY

Computer programs are valuable intellectual property. Software publishers can be very aggressive in protecting their property rights from infringement. In addition to software, legal protections can also exist for any information published on the Internet, such as the text and graphics on a web site. As such, it is important that users respect the rights of intellectual property owners. Users should exercise care and judgment when copying or distributing computer programs or information that could reasonably be expected to be copyrighted.

VI. COMPUTER VIRUSES

Users should exercise reasonable precautions in order to prevent the introduction of a computer virus into the local area or wide area networks. Virus scanning software should be used to check any software downloaded from the Internet or obtained from any questionable source. In addition, executable files (program files that end in ".exe") should not be stored on or run from network drives. It is also recommended that floppy disks be scanned periodically to ensure against infection.

VII. NETWORK SECURITY

As the College's desktop computers are connected to a local network, it is critically important that users take particular care to avoid compromising the security of the network. Most importantly, users are prohibited from sharing their passwords with anyone else, and should promptly notify College computer services personnel if they suspect their passwords have been compromised. In addition, users who will be leaving their PCs unattended for extended periods should either log off the network or have a password-protected screensaver in operation. Further, all computer accounts must be password protected.

VIII. E-MAIL

Users of the College's ITRs for electronic mail purposes shall have no expectation of privacy over any e-mail communications or transmissions sent or received. The College reserves the right to access and/or review any e-mail communications or transmissions for the purpose of enforcing this policy or for other reasons including, but not limited to, routine system maintenance, technical problems or criminal investigations. The College also reserves the right to interrupt a user's service when this policy has been violated or an alleged violation is being investigated. Further, under most circumstances, an e-mail transmission is a public record and must be disclosed when requested pursuant to the Commonwealth's Public Records Law.

IX. NO EXPECTATION OF PRIVACY

All College ITRs are the property of the College and the Commonwealth of Massachusetts and shall be used in conformance with this policy. Users of the College's ITRs shall have no expectation of privacy over any use on the College's ITRs or any communications, work product or information generated as a result of such use. The College retains the right to inspect any user's computer, any data contained in it, and any data sent or received by that computer. Further, users should be aware that in order to ensure proper network operations, network administrators routinely monitor network traffic and that the computer systems automatically record account use information including, times of login and logout, unusual account activity such as failed login attempts, the physical terminal where such attempts are made, and disk storage use. Additionally, College's phone system automatically records the extension, authorization code, and length of connection for all calls.

X. VIOLATIONS

Violations of this policy may result in disciplinary action, up to and including dismissal. Further, a user who violates this policy may be subject to civil and/or criminal liability for violating state or federal laws, including, but not limited to: the Electronic Communications Privacy Act of 1986, the Family Educational Rights and Privacy Act, Massachusetts Wiretap Law, defamation, copyright and/or trademark infringement laws, the Digital Millennium Act or sexual harassment or discrimination laws.

I have read this policy in its entirety, I understand its terms and conditions, and I acknowledge and accept my responsibilities as an authorized user of the College's Information Technology Resources.

______________________________ | ______________________________ ____________________

Applicant's Name (please print)   Applicant's Signature   Date

---

① **Moodle** - BCC's course management system provides tools for placing course materials, assignments, notes, quizzes and tests online.

② **BCC WebAdvisor** accounts are used to access course enrollment, access student info for advising, entering student grades, opting in and out of BCC's Emergency Notification System (ENS)

③ **Long Distance Code** – an **LDC** is need by any adjunct faculty member who wishes to make a long distance call from any of the campus phones.
Copier Code – is used to either print or copy documents to the Xerox multifunction printers on BCC campuses.